Annex "A"

Guidelines on Written Policies and Procedures for DMA TPs

Pursuant to Section 4(c)(ii) of the DMA Rules, TPs who want to offer DMA Services to its clients are required to submit to the Exchange a certification signed by its Nominee, or any of its authorized signatories, stating that the TP has written policies and procedures, which contain, at the minimum, the following:

1. **Risk Management and Supervisory Procedures**

    a. *Reviewing Effectiveness of Risk Management Protocols* – TPs are required to establish, document and maintain a system for regularly reviewing the effectiveness of the risk management controls and supervisory procedures and for promptly addressing any issues.

    b. *Risk Profiling of Clients* – TPs are required to establish the risk profile of their clients. Each type of risk profile should be associated with a set of risk management protocols. The risk profiles should be reviewed regularly to ensure appropriateness of the risk parameters.

    c. *Confirmation of Risk Management Controls* –The Risk Management Officer of the TP or its equivalent officer is required, on a daily basis, to confirm that the risk filters comply with existing regulatory rules and that regular review has been conducted.

2. **Monitoring and Managing of DMA Orders**

    a. TPs shall have a facility to monitor the activities of their DMA Clients.

    b. TPs shall have access to the DMA Orders for the purpose of:

        i. viewing the DMA Order; or
        ii. modifying or cancelling the DMA Order, if requested by the DMA Client.

    c. TPs shall keep a record of all communication logs with DMA Clients, which shall include, without limitation, the following:

        i. date/time;
        ii. name of caller/sender;
        iii. designation/relationship to the account holder (if applicable);
        iv. nature of description of call;
        v. action taken (if any);
        vi. result of action (if applicable);
        vii. name of recipient;
        viii. mode of communication; and
        ix. number/email address used.

3. **Handling of DMA Orders breaching the trading thresholds**

    In cases where a DMA Order breaches the trading thresholds (i.e. static thresholds and dynamic thresholds), the TP shall, upon the request of the Exchange, confirm whether the order is valid or not.

4. Handling of errors and/or exception

a. Any error, rejections, and exceptions shall be monitored and investigated/resolved on a daily basis. A review of the actions taken in relation to errors and/or exceptions shall be undertaken by the Compliance Officer of the TP on a regular basis.

b. The procedure for handling of errors and/or exceptions shall include, but is not limited to, the following:

i. recommended solutions; and
ii.escalation procedures

5. Business continuity and disaster recovery plan

TPs shall have a business continuity and disaster recovery plan to ensure continuity of operations in the event of emergencies or disasters that are likely to cause significant disruption in the provision of DMA Services. The BCP and schedule of the disaster recovery test shall be effectively communicated to the DMA Clients.

6. Validation of identity of the person accessing the DMA Service

a. TPs shall require clients to fill up a long-form Know-Your-Client (KYC) form, detailing therein the manner and method by which the DMA TP clears and authorizes a prospective DMA Client to avail of the DMA facilities.

b. TP shall exercise due diligence in verifying the true and full identity of the DMA Client and its investment objectives and financial situation prior to the provision of DMA Service.

c. TP shall be assured of the financial probity of the DMA Client and that it has sufficient financial resources to meet its obligations.

7. Hiring and training of qualified technical personnel supporting the DMA Service of the TP

TP shall ensure that its technical personnel possess the required skills to address the following system-related issues:

i. Connectivity
ii. Security
iii. Application
iv. Database